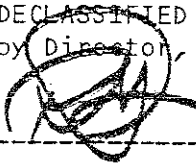


SRH- 213

OFFICE OF OPERATIONS BULLETINS
OFFICE OF CHIEF OF NAVAL OPERATIONS
NAVY DEPARTMENT
1935 - 1941

DECLASSIFIED per Part 3, E.O. 12356
by Director, NSA/Chief, CSS


Date 27 December 1982

REVIEWER'S NOTE:

The first review of this document was conducted by personnel of the U. S. Navy. The original classified versions were retained by them and have been placed in the NSG Repository, Crane, Indiana

CONTENTS

Serial No. 5 -- Cryptography, 15 July 1935. 001
Serial No. 17 - Cryptography, 15 July 1936. 003
Serial No. 18 - Cryptography, 15 August 1936. 005
Serial No. 19 - Cryptanalysis, 15 September 1936. 008
Serial No. 20 - Cryptanalysis, 15 October 1936. 011
Serial No. 21 - Cryptanalysis, 15 November 1936 014
Serial No. 22 - Cryptanalysis, 15 December 1936 016
Serial No. 23 - Cryptanalysis, 15 January 1937. 019
Bulletin No. 65 - Cryptanalysis, 15 January 1941. 021
Bulletin No. 66 - Cryptanalysis, 15 April 1941. 024

RESTRICTED

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON

15 JULY 1935.

- OFFICE OF OPERATIONS BULLETIN -

SUBJECT - CRYPTOGRAPHY - SERIAL No. 5

- REMARKS -

A common fault among beginners in the study of cryptanalysis is the placing of too much weight on the frequencies of individual letters. For instance, "E" has the highest average value in English text, but is not necessarily the letter of highest frequency in a given cryptogram. Re-petitions and peculiar letter distributions are far more important than frequencies and form the basis of all cipher solution.

Peculiar letter distributions are; doubled letters, repeated letters within a small number of letters, reversed digraphs, the combinations of the lowest and highest frequency letters, etc. These permit the assumption of plain-text having the same peculiarities of letter distribution. The assumption may be checked by the frequencies of the letters involved, and verified by substitution of the assumed letters where they occur again in the cryptogram.

Errors are inevitable in the execution of all the operations of cryptographic communications. Such errors are called "garbles", and should be expected occasionally. Garbles are not often introduced deliberately into Bulletin problems, but when they do occur in the finished product they are usually allowed to remain in order to give experience in overcoming this difficulty.

/s/ S. C. Hooper,
Captain, U.S. Navy,
Director of Naval Communications.

By direction.

001

REMAINING PAGES NOT RELEASABLE

NAVY DEPARTMENT
OFFICE OF CHIEF OF NAVAL OPERATIONS
WASHINGTON

1500

~~RESTRICTED~~

15 JULY 1936.

OFFICE OF OPERATIONS BULLETIN
SUBJECT: CRYPTOGRAPHY - SERIAL No. 17

- REMARKS -

The purpose of the Cryptography Bulletin is to locate those officers or men within the Naval service who are interested in cryptography, and to afford them a medium for beginning their instruction.

A special Mailing List is maintained for this Bulletin, and requests from individuals to be placed on this Mailing List are invited.

In each issue of the Cryptography Bulletin there are three cipher problems published. The problems are numbered according to complexity, Problem No. 1 being of an elementary nature, and Problems No. 2 and No. 3 being of a somewhat more advanced type.

A loan library of instructional pamphlets is maintained for use in connection with the solution of Bulletin problems. All correspondence relative to this Bulletin, such as, requests to be placed on the Mailing List, request for pamphlets, and the submission of solutions to problems, should be addressed to:

Chief of Naval Operations,
(Communication Security Group)
Navy Department,
Washington, D.C.

Commanding Officers receiving this Bulletin are requested to give it as wide a circulation within their commands as is practicable, with the limitation that publicity connected with this Bulletin should be RESTRICTED to personnel of the Navy or Naval Reserve.

/s/ C. E. Courtney,
By direction.

REMAINING PAGES NOT RELEASABLE

NAVY DEPARTMENT
OFFICE OF CHIEF OF NAVAL OPERATIONS
WASHINGTON

~~RESTRICTED~~

15 AUGUST 1936

OFFICE OF OPERATIONS BULLETIN
SUBJECT: CRYPTOGRAPHY - SERIAL No. 18

- REMARKS -

The number of solutions submitted for the July problems was markedly below normal, although the problems were no more difficult than usual. It is hoped that this was caused more by heavy schedules than by a diminished interest. This office will welcome any suggestions for improvement in the Bulletin; these may be included with solutions submitted.

It is felt that many students on the mailing list are not obtaining full value from the Bulletin because they submit solutions irregularly. This causes difficulties when a series of problems is presented, for quite often one of the cryptograms might look hopeless, whereas, had the problem for the preceding month been attacked, a hint concerning the general type of cipher employed might have been obtained. It is surprising how rapidly the technique slips away from the cryptanalyst who takes a vacation from it, and how large a part continuity plays in the successful solution of ciphers. For these reasons, it is believed that regularity will be of great help to progress.

From time to time the question arises as to whether it is advisable for beginners to attempt solution of the No. 2 and No. 3 problems. The No. 1 problems are always of an elementary type, and, as such, serve as an introduction to the general technique of solution. The No. 2 problems are of a more complex nature, but their solution depends more upon ingenuity than experience, and the beginner is by no means wasting his time in attempting their solution. Ordinarily, the solution of the No. 3 problems requires not only ingenuity but also a certain amount of experience. Beginners, therefore, should not spend too much time on these problems until they feel well grounded in fundamentals. In addition, a former policy of giving No. 3 problems in a series extending over three or four months is to be reinaugurated. Successful attack on a problem will be greatly dependent upon the knowledge of the system gained from the solution of the preceding problems. Therefore, all students, in addition to beginners, are advised to attack each No. 3 problem of a series in succession.

/s/ C. E. Courtney,
By direction

(RETYPE FOR PURPOSE OF CLARITY)

005

REMAINING PAGES NOT RELEASABLE

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON

RESTRICTED

15 September 1936.

OFFICE OF OPERATIONS BULLETIN

SUBJECT: CRYPTANALYSIS - SERIAL No. 19

REMARKS

The novice in cryptanalysis is at first bewildered because he cannot visualize the complete process of solution. Often he does not even know how to start and wants instructions. Later he becomes disgusted when his first assumptions turn out wrong. Everyone must learn that "there is no royal road to cryptography". The method of solution depends on the cipher or on the cryptogram and not on the cryptanalyst.

For the purpose of illustration, cipher solution might well be compared to mountain climbing. Anyone with a strong back and a good guide can get to the top of the average mountain, especially if he is roped between two guides. But this does not qualify him as a mountain climber, even if he goes up the same trail a hundred times. Take his guide away and put him on a different mountain, and he will (probably) end in disaster. On the other hand, put the guide on a strange mountain and he will safely wind his way to the top. What is the cause of the one failing while the other succeeds?

In the first place the guide, a professional, has that intangible asset known as experience. But experience alone is not enough. Frederick the Great's team of mules had been through twenty campaigns, but they were still mules. We must, therefore, attribute the success of the expert mountaineer to a thorough understanding of the basic principles of mountain climbing.

These basic principles are few in number and extremely simple. The actual difficulty of a climb is usually much different from the apparent difficulty. Telescopic examination of a sheer cliff will reveal ledges, outcroppings, and holes which will give the mountaineer some tangible factor to work with. Closeup inspection will discover cracks and crevices which afford a hold. A hand hold is not much - certainly for the beginner - but it is all there is, and it has to suffice. And these cracks can always be found if one knows how to look for them. Also, there are dangers to be avoided such as weathered rock, land slides, ice, snow, and crevasses.

REMAINING PAGES NOT RELEASABLE

~~RESTRICTED~~

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON

15 OCTOBER 1956.

*

OFFICE OF OPERATIONS BULLETIN
SUBJECT: CRYPTANALYSIS - SERIAL No. 20

* REMARKS *

The purpose of this Bulletin is to create a group of amateur cryptanalysts within the Naval service by locating those interested in cryptanalysis and affording them an opportunity for instruction.

A special Mailing List is maintained for this Bulletin, and requests from individuals to be placed on this Mailing List are invited.

In each issue of the Cryptanalysis Bulletin there are three cipher problems published. The problems are numbered according to complexity, Problem No. 1 being of an elementary nature, and Problems No. 2 and No. 3 being of a somewhat more advanced type.

A loan library of instructional pamphlets is maintained for use in connection with the solution of Bulletin problems. All correspondence relative to this Bulletin, such as requests to be placed on the Mailing List, requests for pamphlets, and the submission of solutions to problems, should be addressed to:

Chief of Naval Operations (Communication Security Group).

Commanding Officers receiving this Bulletin are requested to give it as wide a circulation within their commands as is practicable. It is especially desired that the Bulletin reach the hands of all newly commissioned officers. The publicity connected with this Bulletin and the Bulletin itself should be RESTRICTED to the officer and enlisted personnel of the Navy and Naval Reserve.

/s/ C. E. Courtney,
By direction.

(RETYPE FOR PURPOSE OF CLARITY)

011

REMAINING PAGES NOT RELEASABLE

NAVY DEPARTMENT
OFFICE OF CHIEF OF NAVAL OPERATIONS
WASHINGTON

~~RESTRICTED~~

15 NOVEMBER 1936.

OFFICE OF OPERATIONS BULLETIN
SUBJECT: CRYPTANALYSIS - SERIAL No. 21

* REMARKS *

The October issue of the Bulletin, in addition to its regular distribution, was mailed as an appendix to the Communications Bulletin and distributed to all ships and stations throughout the Naval Service. The existence of and manner of utilizing the special mailing list was explained under remarks in this issue. This resulted in a sizeable number of applications from members of the Service to be placed on the special mailing list and to receive the instruction pamphlets for beginners.

The attention of all, particularly of beginners, is invited to the RESTRICTED classification of this Cryptanalysis Bulletin. This classification means that the information contained in the Bulletin, and the fact that such a Bulletin exists, should be limited to members of the U.S. Navy and Naval Reserve.

/s/ C.E. Courtney,
By direction.

014

REMAINING PAGES NOT RELEASABLE

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON

RESTRICTED

15 December 1936.

OFFICE OF OPERATIONS BULLETIN

SUBJECT: CRYPTANALYSIS - SERIAL No. 22

- REMARKS -

Since 1900, scientists, sponsored by the Smithsonian Institution, the National Geographic Society, and other similar organizations, have undertaken the study of tree rings based on the hypothesis that the sun affects weather and weather affects trees, hence there is expectation of finding a history of sun-spot variations and weather in the annual rings of trees. By patience, sound analytical reasoning, and, gradually, by experience, an uninterrupted record of weather, rainfall, and sun-spots has been built up which dates back to 700 A.D. This was accomplished by establishing precise dating of rings of living trees, carefully matching overlapping rings of stumps, living trees, and timber, and by analysis of long-continued sequences of what appeared to be the 11-year solar cycle.

This successful study brought forth important revelations in other sciences. It established the accurate dating of over seventy five historical ruins in Arizona; it dated and explained several mass migrations of Pueblo Indian tribes; it throws light on the recently spotlighted subject of soil erosion; it establishes the hypothesis of a three hundred year weather cycle, with a severe drought every hundred years and an extreme drought every three hundred. The record clears up the mystery of the abandoned Pueblo ruins. When discovered by the Spaniards, the long-abandoned ruins showed unmistakable evidence of having been vacated in great haste. For years it was thought that all inhabitants had been annihilated in a great battle and their corpses destroyed. The tree ring record discloses, however, that, in the midst of a great drought, when the water supply was exhausted, the whole community was forced to move in order to survive. With a continuation of the drought, they never returned to their former dwelling.

The information contained in the tree rings has been hidden for many years. It has been there waiting to be uncovered. Likewise, a cryptogram contains hidden information which can also be uncovered by proper analysis. As in the tree ring study, the information is disclosed by scrutiny of the cryptogram itself.

REMAINING PAGES NOT RELEASABLE

NAVY DEPARTMENT
Office of Chief of Naval Operations
WASHINGTON

RESTRICTED

15 January 1937.

OFFICE OF OPERATIONS BULLETIN
SUBJECT - CRYPTANALYSIS - SERIAL No.23

* REMARKS *

In 1925 a limited number of copies of the War Department publication "Elements of Cryptanalysis" were obtained and distributed to various ships, stations, and individuals for permanent use. The publication has long since been out of print and no further copies are obtainable. Requests for the loan of this book are continually being received. These requests cannot be completely filled, even on a loan basis, with the few remaining copies now at hand. Therefore it is desired that individuals who possess personal copies and who no longer require them, return them to the Office of Chief of Naval Operations (Communication Security Group) in order that they may be loaned to students beginning the study of cryptanalysis.

In the Bulletin each month the training pamphlets available for loan are listed. More pamphlets could appear on this list if students returned those loaned promptly at the expiration of the time limit.

/s/ C. E. Courtney;
By direction.

REMAINING PAGES NOT RELEASABLE

NAVY DEPARTMENT
Office of the Chief of Naval Operations
WASHINGTON

Op-20-GR

15 January 1941

OFFICE OF CHIEF OF NAVAL OPERATIONS BULLETIN

SUBJECT -- CRYPTANALYSIS --- BULLETIN No. 65

REMARKS

At the present time the Communication Security Section has sufficient personnel of the Regular Navy taking the Elementary Course in Cryptanalysis and does not desire further requests, except as follows:

- I. Officers or rated men detailed to Coding Boards.
- II. Men possessing special language qualifications or superior education who desire training in cryptanalysis.

It is desired to increase the enrollment of Reserve Enlisted Personnel with the object of creating a group who will be trained and available in event of war.

Applicants should submit their requests via official channels. For men not on Coding Boards, the request must list their educational qualifications, typing ability, language qualifications and any other training or experience which would be of value. Forwarding endorsement of the Commanding Officer should make recommendation of approval or disapproval and should state the reason for enrollment. No action will be taken on applications that are forwarded without a recommendation.

The course is not open to personnel below petty officer rating, except in unusual circumstances, and is not open to anyone on Foreign Station.

LEIGH NIXES,
By direction.

(RETYPE FOR PURPOSE OF CLARITY)

021

REMAINING PAGES NOT RELEASABLE

Op-20-G

NAVY DEPARTMENT
Office of the Chief of Naval Operations
WASHINGTON

~~RESTRICTED~~

15 April 1941

OFFICE OF CHIEF OF NAVAL OPERATIONS BULLETIN

SUBJECT -- CRYPTANALYSIS --- BULLETIN No. 66

REMARKS

Due to the increase in correspondence with students enrolled in the Elementary Course in Cryptanalysis, it is not feasible to continue instruction by bulletin. Therefore, the Cryptanalysis Bulletin will be discontinued with this issue.

LEIGH NOYES,
By direction.

ONE PAGE NOT RELEASABLE

BASIC PRINCIPLES OF CRYPTANALYSIS

✓ 1. Introduction (Subject - The text-book)

✓ 2. Poe.

✓ 3. Training Methods.

✓ 4. Normal Rate of Progress.

5. Hitt.

6. French Writers.

7. Bulletin Problems. (?) (gables)

8. Ciphers.

9. Language. *words sentences - multiplicity of*

10. Collateral Information.

11. Psychology.

12. Hunches vs Orderly Reasoning. *

13. Inspiration, Clues, Breaks.

14. Technique.

15. Definitions of Terms. *(Defined by ...)*

16. Pamphlets. (?) **

17. *assumptions - known words*

18. *Confidence*

19.

20. *List of Basic Principles*

X J. Rives Childs.

* Intuition - Aristotle.

(Pamphlets - Dont hesitate to write us - it is only way to effect improvement.)

Difficulties - unlock our own minds and render in logical order
discover the students mental reactions and his needs.

INTRODUCTION

P The basic principles of cryptanalysis are extremely simple: the difficulty arises in their application. It is somewhat analagous to golf. The principles of any shot are simple enough but hours ~~of practice~~ of practice (plus golfing instinct) are required to master it.

P Suggestions, in substance as follows, have been frequently submitted: -

"Why does not the Navy Department publish a text-book on cryptanalysis, covering all types of ciphers, which I could study. I am very interested in the subject but I do not know enough about ciphers to be able to solve the ^{more} difficult problems." [^]
~~published in the [unclear]~~

~~This idea seems logical enough but it is wrong for one reason: -~~

~~Code and Cipher Solution is an Art - not a Science.~~

← There are several reasons for not publishing such a text-book, the most important being:

- (1) A text book ~~of this type~~ ^{that is suggested} would be of no practical value, ~~but~~ ^{it is not practical}
- (2) The ciphers of the past ("classical" systems) have been fairly well covered in other publications; our present ciphers cannot be described for obvious reasons; and the ciphers of the future are still to be invented.

- (3) A text-book, if written at the present time, would be inadequate in many respects for the simple reason that we do not know its ^{exact} requirements. For example: - ←

"Elementary Cipher Solution" had to be rewritten five

to not incident here

TIMES (AND A NEW PROBLEM SUBSTITUTED) IN ORDER TO MEET THE QUESTIONS ASKED BY A DOZEN OFFICERS. EACH NEW READER WOULD PROBABLY LIKE SOMETHING ADDED FOR HIS OWN BENEFIT.

on cipher solution
A SORT OF TEXT-BOOK IS BEING WRITTEN, BUT IT IS PUBLISHED IN SECTIONS IN THE FORM OF PAMPHLETS. THESE ARE PREPARED TO MEET THE REQUIREMENTS OF THE MOMENT RATHER THAN IN SYSTEMATIC ORDER. * FROM THE REACTIONS OF THE STUDENTS TO THESE PAMPHLETS, THE COMMENTS AND QUESTIONS ASKED, WE ARE LEARNING AS MUCH ABOUT METHODS OF INSTRUCTION AS THE STUDENTS ARE ABOUT METHODS OF SOLUTION. ** (add)

FOR A COMMUNICATION OFFICER WHO NEEDS ONLY A SMATTERING OF CRYPTOGRAPHY, THE PRESENT WAR DEPARTMENT PUBLICATION "ELEMENTS OF CRYPTANALYSIS" IS SATISFACTORY. THIS BOOK MAKES A BRIEF STUDY OF CIPHERS AND CODES AND DESCRIBES SOME OF THE METHODS BY WHICH THEY ARE BROKEN. IT GIVES THESE OFFICERS AN UNDERSTANDABLE (BUT SOMEWHAT INCORRECT) IDEA OF THE WAY IN WHICH SOLUTION IS ACCOMPLISHED AND THUS REMOVES CRYPTANALYSIS FROM THE FIELD OF "BLACK MAGIC". OFFICERS STUDYING THIS PUBLICATION WILL LEARN ENOUGH TO USE OUR CODES AND CIPHERS MORE INTELLIGENTLY. TO QUOTE FROM THE FIRST SECTION OF THIS PUBLICATION: -

"THE PRINCIPAL AIM IN THIS PAMPHLET IS TO SUBJECT THE MORE COMMON TYPES OF CIPHER SYSTEMS TO A CAREFUL SCRUTINY, TO POINT OUT THE EASE WITH WHICH CERTAIN TYPES ARE ANALYZED, OR THE DIFFICULTY WITH WHICH OTHER TYPES ARE SOLVED, AND THUS TO DEMONSTRATE BY INFERENCE SOME OF THE REASONS FOR THE ADOPTION OR REJECTION OF CERTAIN SYSTEMS BY THE SIGNAL CORPS."

FOOTNOTE: SYSTEMATIC ORDER WOULD TEACH THE STUDENT TO EXPECT WHAT HE WILL NOT FIND IN PRACTICE. THE ~~correct~~ ORDER OF PRESENTATION IS NOT KNOWN AND PROBABLY IS NOT IMPORTANT.

*By the way, the order of presentation is not important...
by the order of signal section...
messages in...
afterwards...
method...*

However, for an officer who desires to become really proficient in cipher solution, the above text-book (or any other text-book yet published) is entirely inadequate. In fact, text-books on ciphers are worse than that, they are positive detriments.

This naturally raises the question, - "How is one to learn cipher-solution by himself if he is not permitted a text-book?" The complete answer is rather involved but it may be summarized as follows: - "There is no royal road to cryptography". Cipher-solution can be learned only through the actual solution of cipher messages (problems). Such hints or suggestions as may be obtained from the pamphlets will help the student over the difficult places, but it must be clearly understood that cryptography is an ART - not a SCIENCE. Cryptanalysis cannot be "studied" - it must be absorbed. We can only point out the way - the student must find the path for himself.

2.

POE

Edgar Allan Poe may be termed the prophet of cryptanalysis. *He was a century ahead of his time.* His essay on "CRYPTOGRAPHY", published in 1841, is of more practical value than all the text books ever written. Here is the essence of what he says:

"The BASIS of the whole *art* of cipher solution is found in the general principles of the formation of LANGUAGE itself, and thus is altogether INDEPENDENT of the particular laws which govern any CIPHER, or the construction of its KEY."

"It may be soundly asserted that human ingenuity cannot concoct a cipher which human INGENUITY cannot resolve."

"In the facility with which such writing is deciphered there exists very remarkable differences in different intellects. It may be observed generally that in such investigations the analytical ability is very forcibly called into action."

"If, however, there should be sought in ~~the~~ treatises, ~~or in any~~ RULES FOR THE SOLUTION OF CIPHER, the seeker will be disappointed. Beyond some hints in regard to the general structure of language, and some minute exercises in their practical application, he will find nothing upon record which he does not in his own intellect possess."

The secret basis of the cipher is the structure of language. It is not a matter of chance, but a matter of necessity. The key to the cipher is the key to the language.

HOW POE ARRIVED AT THESE CONCLUSIONS WE DO NOT KNOW, *unless!*

~~POE'S~~ THE INSIGHT OF HIS GENIUS REVEALED THEM AS TRANSCENDENT.

HIS EXPERIENCE WAS LIMITED TO ELEMENTARY CIPHER SYSTEMS ON THE WHOLE, AND NONE APPROACHED THE COMPLEX SYSTEMS OF THE PRESENT DAY. NEVERTHELESS THE TEST OF TIME HAS PROVED ~~THE~~ *his* STATEMENTS TO BE CORRECT. *

AN INTERESTING CONFIRMATION OF THE LAST QUOTATION FROM POE CAN BE FOUND IN A BOOK BY A NOTED FRENCH CRYPTOGRAPHER:

"THE LITERATURE ON CRYPTOGRAPHY IS VERY VOLUMINOUS; IT WOULD BE SCARCELY POSSIBLE TO MENTION IN THESE PAGES THE TITLES OF ALL THE WORKS WHICH HAVE BEEN PUBLISHED ON THIS SUBJECT. I NEED SAY NO MORE THAN THAT, OF ALL THOSE I HAVE READ, THE MOST SUBSTANTIAL IS THE WORK OF A FRENCHMAN. I MIGHT MENTION ALSO THE NAME OF VON KASISKI, A GERMAN MAJOR. BOOKS, IT IS TRUE, PROVIDE A GREAT DEAL OF INTERESTING MATERIAL, BUT THEY DO NOT HELP TO DECIPHER DOCUMENTS WHICH ARE IN ANY DEGREE COMPLICATED, ANY MORE THAN THE BEST OF GRAMMARS CAN MAKE A GOOD WRITER."

* FOOTNOTE: - WE ADHERE TO THIS CONCLUSION DESPITE THE FACT THAT MANY CIPHERS HAVE NEVER BEEN SOLVED. THE ONLY THING DEFINITELY PROVED IS THAT THE PEOPLE WORKING ON THESE SYSTEMS WERE UNABLE TO SOLVE THEM.

Cryptanalysts who attempted to teach cipher solution during the World War have, without exception, complained of the lack of "cipher brains" in their students and of the poor results achieved by these students when they attempted the actual solution of military ciphers. They contrast their own skill and proficiency with that of their students and add to this the fact that they had no text-books and had to work out everything for themselves. There is just one thing they overlooked - THE TRAINING WAS WRONG RATHER THAN THE STUDENTS. The principal reason for the success of the expert cryptanalysts (both American and foreign) was ^{the fact} that they HAD worked out everything for themselves.

Self-instruction in cipher solution (without text@books) has necessarily required groping from the UNKNOWN towards the KNOWN - in other words INDUCTIVE REASONING, just what is required in advanced work. The cryptanalyst progressed from simple to complex systems as the ciphers in actual use became more difficult, but each step represented a new and unknown element.

With the text-books or with class instruction, the process has been the exact opposite; DEDUCTIVE REASONING, working from the KNOWN to the UNKNOWN, and always following ^a logical sequence. First a cipher is described, then its characteristics and earmarks are explained, and finally a few problems in that cipher are given. Meanwhile, the students are busy cultivating bad habits and the wrong point of view. As soon as faced with a real cipher (not in a problem) they are perplexed. It is not in the book and they do not even know how to begin.

The first steps in cryptanalysis are by far the most important.

on account of the habits formed

~~"Give me the child until it is five years old", said the old Jesuit,
"after that you may do with it what you will"~~

How did these older and expert cryptanalysts learn about ciphers? By the simple process of solving cipher messages and then reconstructing the cipher systems used. And that is the very process which is being attempted in the Bulletin problems; - to teach general principles of cryptanalysis, to cultivate INDUCTIVE REASONING, and to ignore the type of cipher except as reconstructed during solution of the cryptogram.

Of course in practice we would be only too glad to discover the ear-marks of a "classical" cipher or other well known system. We may encounter a system which remains effective for a year or more after the initial solution has been achieved. Subsequent solutions of the various keys are always much easier than the initial solution, and various short cuts can be developed. Problems are given which cover these phases of the work. This, however, does not detract from the necessity of basing all training upon INGENUITY and INDUCTIVE REASONING.

No matter how advanced the student may be, the elementary problems should not be despised. They are like setting-up exercises and give a great deal of training for the time and labor involved. No two solutions are exactly alike, and as Kipling expresses it: -

[~~and~~ The things that you learn from the yellow and brown
← Will help you a heap with the white!

The simple substitution ciphers should be solved by inspection. This affords training to both eye and memory.

The importance of the early training, and the acquisition of skill and technique, cannot be too strongly stressed. The writer's own experience in this matter ^{several} ~~seven~~ years ago serves as an example.

He studied the "Army Training Course", working all the problems; then he solved the cryptograms in the "Riverbank Training Course"; finally he was confronted with an actual cipher message. He soon discovered that he was full of theory but devoid of skill or real knowledge of cipher solution. Concentration on elementary problems effected the cure.

The suspicion that something might be wrong with the training course did not arise for several years. Unfortunately, too many who took these courses never discovered the reason for their failure or did not stay in the game long enough to UNLEARN what they had been taught.

The proportion of humanity endowed with "cipher brains" has been estimated to be from one in a thousand to one in a million. Our own experience with officers of the Navy would indicate that this proportion may be as high as four or five percent.

4. Normal RATE OF PROGRESS

IF THE STUDENT DOES NOT DEVELOP A CIPHER "INFERIORITY COMPLEX" AT AN EARLY DATE HE IS DIFFERENT FROM THE ORDINARY RUN OF MORTALS, OR ELSE OUR PRESENT TRAINING METHODS ARE GREAT IMPROVEMENTS OVER THOSE OF THE PAST.

IT SHOULD BE REALIZED THAT THERE IS NO SUCH THING AS "INTENSIVE TRAINING" IN CRYPTANALYSIS. PROGRESS AT THE START IS ALWAYS WOEFULLY SLOW. THE WHOLE SUBJECT IS SO FOREIGN TO OUR NORMAL MENTAL PROCESSES THAT THE SUB-CONSCIOUS MIND SEEMS TO OPPOSE IT. IT WILL SINK IN ONLY BY DEGREES. INDEED, WE LEARN MORE BY ABSORPTION THAN BY CONSCIOUS EFFORT. IT IS UNWISE TO WORK TOO HARD OR TOO LONG: AFTER ABOUT THREE HOURS THE BRAIN REBELS AND QUILTS WORKING. IT IS BEST TO STOP AT THE END OF TWO HOURS AND RESUME THE SOLUTION TWENTY FOUR HOURS LATER. IT TAKES A LONG TIME TO "HARDEN" A CRYPTANALYST TO THE POINT WHERE HE CAN WORK ALL DAY.

THE FIRST STEPS IN CRYPTOGRAPHY, BY FAR THE MOST IMPORTANT AS REGARDS FUTURE PROGRESS, ARE THUS BOTH SLOW AND DIFFICULT. HOWEVER, CONTINUED WORK ON ELEMENTARY PROBLEMS WILL FINALLY GET THE STUDENT THROUGH THIS PAINFUL STAGE. WHEN HE IS ABLE TO SOLVE A SIMPLE SUBSTITUTION CIPHER WITH EASE, HE IS READY TO STEP OUT AND TACKLE THE MORE ADVANCED PROBLEMS.

THE ELEMENTARY PROBLEMS IN BOTH TYPES OF CIPHERS (SUBSTITUTION AND TRANSPOSITION) MAY BE WORKED ON CONCURRENTLY! ONE IS AN AID TO THE OTHER. THERE IS A ~~GOOD~~ REASON FOR THIS - THE LANGUAGE IS THE SAME IN BOTH CASES.

5. HITT

Captain (now Colonel) Parker Hitt, U.S. Army, was the first American to undertake "practical cipher solution", and has never been given the credit he deserves for his pioneer work. Hitt's "Manual for the Solution of Military Ciphers - 1916" was used as a text-book in the U.S. Army during the World War, and is the only text-book yet published of any practical value. It proved to be the despair of logical minds, due to its non-systematic arrangement. Each "case" of solution began with a cryptogram, outlined the steps of solution, and more or less ignored the cipher involved. (The logical mind always wants all the details of the cipher before attempting its solution).

Hitt's Manual had many defects. It was incomplete as it covered only the systems which came under Captain Hitt's observation. It mentioned "vowel classification" several times but failed to state how this was done. It placed too great stress on frequencies. Its treatment of "standard alphabets" is now obsolete, as such systems would be used only by amateurs. Nevertheless, Hitt's Manual was a most important contribution to the literature on cryptography. As the "Manual for the Solution of Military Ciphers" is out of print, certain extracts are quoted herein as a matter of general information.

Introduction

"The history of war teems with occasions where interception of dispatches and orders written in plain language has resulted in defeat and disaster for the force whose intentions thus became known at once to the enemy. For this reason prudent generals have used cipher and code messages from time immemorial."

"It is unnecessary to point out that a cipher which can be deciphered by the enemy in a few hours is worse than useless. It requires a surprisingly long time to encipher and decipher a message, using even the simplest kind of cipher, and errors in transmission of cipher matter by wire or radio are unfortunately too common."

"Kerckhoffs has stated that a military cipher should fulfill the following requirements:

1st. The system should be materially if not mathematically indecipherable.

2d. It should cause no inconvenience if the apparatus and methods fall into the hands of the enemy.

3d. The key should be such that it could be communicated and remembered without the necessity of written notes and should be changeable at the will of the correspondents.

4th. The systems should be applicable to telegraphic correspondence.

5th. The apparatus should be easily carried and a single person should be able to operate it.

5. HITT

Captain (now Colonel) Parker Hitt, U.S. Army, was the first American to undertake "practical cipher solution", and has never been given the credit he deserves for his pioneer work. Hitt's "Manual for the Solution of Military Ciphers - 1916" was used as a text-book in the U.S. Army during the World War, and is the only text-book yet published of any practical value. It proved to be the despair of logical minds, due to its non-systematic arrangement. Each "case" of solution began with a cryptogram, outlined the steps of solution, and more or less ignored the cipher involved. (The logical mind always wants all the details of the cipher before attempting its solution).

Hitt's Manual had many defects. It was incomplete as it covered only the systems which came under Captain Hitt's observation. It mentioned "vowel classification" several times but failed to state how this was done. It placed too great stress on frequencies. Its treatment of "standard alphabets" is now obsolete, as such systems would be used only by amateurs. Nevertheless, Hitt's Manual was a most important contribution to the literature on cryptography. As the "Manual for the Solution of Military Ciphers" is out of print, certain extracts are quoted herein as a matter of general information.

Introduction

"The history of war teems with occasions where interception of dispatches and orders written in plain language has resulted in defeat and disaster for the force whose intentions thus became known at once to the enemy. For this reason prudent generals have used cipher and code messages from time immemorial."

"It is unnecessary to point out that a cipher which can be deciphered by the enemy in a few hours is worse than useless. It requires a surprisingly long time to encipher and decipher a message, using even the simplest kind of cipher, and errors in transmission of cipher matter by wire or radio are unfortunately too common."

"Kerckhoffs has stated that a military cipher should fulfill the following requirements:

- 1st. The system should be materially if not mathematically indecipherable.
2. It should cause no inconvenience if the apparatus and methods fall into the hands of the enemy.
- 3d. The key should be such that it could be communicated and remembered without the necessity of written notes and should be changeable at the will of the correspondents.
- 4th. The systems should be applicable to telegraphic correspondence.
- 5th. The apparatus should be easily carried and a single person should be able to operate it.
- 6th. Finally, in view of the circumstances under which it must be used, the system should be an easy one to operate, demanding neither mental strain nor knowledge of a long series of rules.

"A brief consideration of these six conditions must lead to the conclusion that there is no perfect military cipher. The first requirement is the one most often overlooked by those prescribing the use of any given cipher and, even if not overlooked, the indecipherability of any cipher likely to be used for military purposes is usually vastly overestimated by those prescribing the use of it."

"The cipher of the amateur, or of the non-expert who makes one up for some special purpose, is almost sure to fall into one of the classes whose solution is an easy matter. The human mind works along the same lines, in spite of an attempt at originality on the part of the individual, and this is particularly true of cipher work because there are so few sources of information available. In other words, the average man, when he sits down to evolve a cipher, has nothing to improve upon; he invents and there is no one to tell him that his invention is, in principle, hundreds of years old. The ciphers of the Abbe Tritheme, 1499, are the basis of most of the modern substitution ciphers."

"In view of these facts, no message should be considered indecipherable. Very short messages are often very difficult and may easily be entirely beyond the possibility of analysis and solution, but it is surprising what can be done, at times, with a message of only a few words."

"In the event of active operations, cipher experts will be in demand at once. Like all other experts, the cipher expert is not born or made in a day; and it is only constant work with ciphers, combined with a thorough knowledge of their underlying principles, that will make one worthy of the name."
(Note: This was written in 1916. His prophecy was fulfilled a year later.)

Equipment for Cipher Work

"Success in dealing with unknown ciphers is measured by these four things in the order named; perseverance, careful methods of analysis, intuition, luck. The ability at least to read the language of the original text is very desirable but not essential."

"Cipher work will have little permanent attraction for one who expects results at once, without labor, for there is a vast amount of purely routine labor in the preparation of frequency tables, the rearrangement of ciphers for examination, and the trial and fitting of letter to letter before the message begins to appear."

"The methods of analysis given in these notes cover only the simpler varieties of cipher and it is, of course, impossible to enumerate all the varieties of these. It is believed that the methods laid down are sound and several years of successful work along this line would seem to conform to this belief."

"Under intuition must be included a *Knowledge of the* general situation and, if possible, the special situation which led to the sending of the cipher message. The knowledge or guess that a certain cipher message contains a particular word, often leads to its solution."

Technique of Cipher Examination

"The preamble, "place from," date, address and signature, give the most important clues as to the language of the cipher, the cipher method probably used, and even the subject matter of the message. If the whole of a telegraphic or radio message is in cipher, it is highly probable that the preamble, "place from", etc., are in an operators' cipher and are distinct from the body of the message. As these operators' ciphers are necessarily simple, an attempt should always be made to discover, by methods of analysis to be set forth later, the exact extent of the operator's cipher and then to decipher the parts of the message enciphered with it".

"In military messages, we almost invariably find the language of the text to be that of the nation to which the military force belongs. The language of the text of the message of secret agents is, however, another matter and, in dealing with such messages, we should use all available evidence, both external and internal, before deciding finally on the language used. Whenever a frequency table can be prepared, such a table will give the best evidence for this purpose."

"All work in enciphering and deciphering messages and in copying ciphers should be done with capital letters. There is much less chance of error when working with capitals and with little practice, it is just about as fast. An additional safeguard is to use black ink or pencil for the plain text and colored ink or pencil for the cipher. A separate color may be used for the key when necessary."